Exhibit "A"

ERIC A. GROVER (SBN 136080)
eagrover@kellergrover.com
ROBERT W. SPENCER (SBN 238491)
rspencer@kellergrover.com
KELLER GROVER LLP
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861

TODD GARBER (*pro hac vice* application forthcoming)
tgarber@fbfglaw.com
ANDREW C. WHITE (*pro hac vice* application forthcoming)
awhite@fbfglaw.com
FINKELSTEIN, BLANKINSHIP
FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, NY 10601
Telephone: (914) 298-3287
Facsimile: (914) 908-6724

Attorneys for Plaintiff
XAVIER NEAL-BURGIN

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

XAVIER NEAL-BURGIN, on behalf of himself, and all others similarly situated,

Plaintiff,

v.

HOUSING AUTHORITY OF THE CITY OF LOS ANGELES.; and DOES 1 through 50, inclusive,

Defendants.

Case No: 23STCV06494

CLASS ACTION

CLASS ACTION COMPLAINT FOR DAMAGES AND RESTITUTION

DEMAND FOR JURY TRIAL

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

Plaintiff Xavier Neal-Burgin, individually and on behalf of all other similarly situated persons, by and through his attorneys, as and for his class action complaint against defendant Housing Authority of the City of Los Angeles, respectfully alleges, upon his own knowledge or, where he lacks personal knowledge, upon information and belief including the investigation of his counsel, as follows:

INTRODUCTION

1. Plaintiff Xavier Neal-Burgin("Plaintiff") bring this class action lawsuit on behalf of himself and all other similarly situated persons against defendant Housing Authority of the City of Los Angeles ("Defendant" or "HACLA") as a result of Defendant's failure to safeguard and protect the confidential information of Plaintiff and the other members of the Class -- including Social Security Numbers and personal information that can be used to perpetrate identity theft -- in Defendant's custody, control, and care (the "Sensitive Information").

2. Plaintiff is an applicant for housing with HACLA. As a condition of submitting an application with HACLA Plaintiff was required to and did supply Sensitive Information to Defendant, including, but not limited, to his Social Security Number, date of birth, driver's license or state identification number, and other personal private data.

3. Unbeknownst to Plaintiff, Defendant did not have sufficient cyber-security procedures and policies in place to safeguard the Sensitive Information it possessed. As a result, between January 15, 2022 and December 31, 2022, cybercriminals were able to access certain HACLA computer systems, thereby gaining access to approximately a massive trove of 15 terabytes of Class Members' Sensitive Information, including Plaintiff's, stored in those systems (the "Data Breach"). Plaintiff and members of the proposed Class have suffered damages as a result of the unauthorized and preventable disclosure of their Sensitive Information.

4. The infamous criminal group LockBit, a hacker collective known for numerous data security attacks, claimed to have perpetrated the Data Breach. On December 31, 2022 LockBit published Class Members' Sensitive Information on the dark web, where it can be used to facilitate identity theft and other fraud.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

5. Plaintiff has received significantly more spam texts, calls, and emails since the Data Breach.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity protections and protocols that were necessary to protect the Sensitive Information of students and employees entrusted into Defendant's custody and care.

7. This lawsuit seeks to redress Defendant's unlawful disclosure of the Sensitive Information of all persons affected by this Data Breach.

8. Plaintiff asserts causes of action sounding in common negligence, negligent hiring and training of employees, breach of duty, and delay in notification of the Data Breach, all arising from Defendant's failure to safeguard his Sensitive Information, and brings claims for consequential damages, injunctive relief, and punitive damages.

PARTIES

9. Xavier Neal-Burgin is a natural person residing in Los Angeles, California. He is a citizen of California.

10. Defendant Housing Authority of the City of Los Angeles is a California state-chartered agency providing affordable housing and job training to low-income residents in the city of Los Angeles, California.

11. At all times material hereto, HACLA acted by and through agents, employees, and representatives, who were acting in the course and scope of their respective agency or employment and/or in the promotion of Defendant's business, mission, and/or affairs.

JURISDICTION AND VENUE

12. This class action is brought pursuant to California Code of Civil Procedure § 382. The damages sought by Plaintiff will be established according to proof at trial.

13. This Court has jurisdiction over all causes of action pursuant to the California Constitution, Art. VI, § 10.

14. This Court has jurisdiction over Defendant because, upon information and belief, Defendant is a citizen of California, has sufficient minimal contacts in California, or otherwise

intentionally avails itself of the California market so as to render the exercise of jurisdiction over it by the California courts consistent with traditional notions of fair play and substantial justice.

15. Venue is proper in this court because Defendant is located in Los Angeles County, and Los Angeles County is the location where a substantial part of the events or omissions giving rise to Plaintiff's claims occurred.

THE RISKS OF DATA BREACHES AND COMPROMISED SENSITIVE INFORMATION ARE WELL KNOWN

16. Defendant had obligations created by contract, industry standards, common law, and representations made to current, former, and prospective students to keep Plaintiff's and Class Members' Sensitive Information confidential and to protect it from unauthorized access and disclosure.

17. Defendant's data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported on in the last few years. In fact, in the wake of this rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies and institutions that maintain individuals' Sensitive Information.[1]

18. Indeed, according to a report by Risk Based Security, Inc., by the end of June, 2020 was already the "worst year on record" in terms of records exposed in data breaches.[2]

19. Therefore, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensure that adequate protections were in place.

/ /

/ /

/ /

[1] *See, e.g., Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[2] *See 2020 Q3 Report*, Risk Based Security, *available at* https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

DEFENDANT ALLOWED CRIMINALS TO OBTAIN PLAINTIFF'S AND THE CLASS' SENSITIVE INFORMATION.

20. Plaintiff and Class Members were obligated to provide Defendant with their Sensitive Information as part of their relationships with Defendant.

21. Due to inadequate security against unauthorized intrusions, cybercriminals breached Defendant's computer systems between approximately January 15, 2022 and December 31, 2022. This Data Breach resulted in the criminals unlawfully obtaining access to current and former applicants' Sensitive Information, including their identities and Social Security Numbers.

DATA BREACHES LEAD TO IDENTITY THEFT

22. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[3]

23. Indeed, the LockBit hacker collective has already posted Sensitive Information of Class Members on the dark web, where it can be purchased and used by malicious actors to commit a variety of fraud, including but not limited to identity theft.

24. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[4] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[3] *See* https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/ (last accessed May 7, 2019).

[4] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited June 3, 2019).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

25. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[5]

26. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

27. There may be a time lag between when sensitive information is stolen and when it is used. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

28. With access to an individual's Sensitive Information, cyber criminals can do more than just empty a victim's bank account -- they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[7]

29. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and

---

[5] *Id.* at 2, 9.

[6] *Id*. at 29 (emphasis added).

[7] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 28, 2019).

cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other Sensitive Information directly on various Internet websites making the information publicly available.

DEFENDANT DELAYED NOTICE TO PLAINTIFF AND THE CLASS

30. Despite becoming aware of the Data Breach on or about December 31, 2022, Defendant only notified Plaintiff and members of the Class that its systems had been breached and that their Sensitive Information was compromised in March, 2023 -- months after Defendant learned that the Data Breach occurred.

31. On or about March 10, 2023, Defendant sent letters to Plaintiff and other Class members advising them that their Sensitive Information had been subject to unauthorized access and had been compromised on or about January 15, 2022 through December 31, 2022 (the "Letter Notification"). A copy of the Letter Notification that Plaintiff received is attached as Exhibit A to this Complaint. The Letter Notification offered only a single year of credit monitoring through Experian IdenityWorks, and only for individuals who signed up for such monitoring by June 30, 2023.

DEFENDANT'S OBLIGATIONS AND ITS NEGLIGENT FAILURE TO MEET THEM

32. In the ordinary course of, and as a condition of, applying for housing assistance with HACLA, Plaintiff, like thousands of other current and former applicants provided Sensitive Information, including but not limited to his Social Security Numbers, to Defendant.

33. Defendant maintains this Sensitive Information within its data infrastructure.

34. Defendant compounded the actual and potential harm arising from the Data Breach by not notifying Plaintiff and other Class Members of the compromise of their personal information until March 2023, when the Letter Notification was sent. Defendant's own Letter Notification advises Plaintiff and other Class Members to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity".[8] Defendant's unjustified delay in notifying Plaintiff and the

[8] *See* Notice Letter

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

Class that they were victims of the Data Breach will dilute any salutary effect that might come from these suggestions.

35. Defendant's security failure demonstrates that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiff's and the Class Members' Sensitive Information;

c. Properly monitoring its own data security systems for existing intrusions; and

d. Ensuring that agents, employees, and others with access to Sensitive Information employed reasonable security procedures.

36. Plaintiff and all members of the Class have consequently suffered harm by virtue of the compromise and exposure of their Sensitive Information -- including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) a loss of privacy. Plaintiff and Class Members were also injured because they did not receive the full value of the services for which they bargained; to wit, educational services plus adequate data security. Plaintiff and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identify theft and the attendant dangers thereof for the rest of their lives because their Sensitive Information, including Social Security Numbers, is in the hands of cyber-criminals.

DEFENDANT'S INADEQUATE RESPONSE TO THE DATA BREACH

37. Defendant's Letter Notification stated that it is "reviewing [HACLA's] policies and procedures relating to data privacy and security."[9] No details were provided, and thus it cannot be determined from the Letter Notification whether Defendant did any of the foregoing, or if it did, whether these enhancements are sufficient to prevent recurrences similar to the Data Breach.

[9] *See* Letter Notification at 1.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

38. The belated Letter Notification also included an offer from Defendant of one year of free credit monitoring and identity theft resolution services through a third party provider, Experian. Defendant, however, offered an unreasonably short window of opportunity to claim these services, with victims of the Data Breach needing to claim these services before June 30, 2023, or be closed out. In addition, one year of credit monitoring services is insufficient, given that Plaintiff's and the Class Members' risk of identity theft will continue throughout their lives.

39. Conspicuously absent from the Letter Notification is any offer of compensation for out-of-pocket losses which the Class has and foreseeably will sustain -- including, but not limited to, time spent to rectify any and all harms that resulted from the Data Breach. Plaintiff and members of the Class have suffered financial loss, including but not limited to lost opportunity costs for the time and effort necessary to remedy the harm they suffered. Thus, Defendant's offer in the Letter Notification fails to make Plaintiff and the other members of the Class whole.

CLASS ALLEGATIONS

40. This action is brought on behalf of Plaintiff and all similarly situated persons pursuant to Cal. Civ. Proc. Code § 382. The Class is defined as:

> All persons whose Sensitive Information was exposed to unauthorized access by way of the data breach of Defendant's computer system between approximately January 15, 2022 and December 31, 2022.

41. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

42. Plaintiff is a member of the Class.

43. Excluded from the Class are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers, directors, and employees of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

44. This action seeks both injunctive relief and damages.

45. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

46. **Numerosity of the Class.** On information and belief, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

47. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendant's data security systems prior to the Data Breach met industry standards;

c. Whether Plaintiff's and other Class Members' Sensitive Information was compromised in the Data Breach; and

d. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

48. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

49. **Adequacy.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

50. Plaintiff and his chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") and Keller Grover LLP -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

51. FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

52. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

53. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only MSMC current and former students and employees, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

54. In addition, Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or equitable relief with respect to the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE IN THE HANDLING OF
PLAINTIFF'S AND THE CLASS' SENSITIVE INFORMATION

55. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

56. Defendant owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff's and Class Members' Sensitive Information within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over its computer systems and network so as to prevent unauthorized access thereof.

57. Defendant owed a duty of care to the Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its computer systems adequately protected the Sensitive Information of the individuals who entrusted it to the Defendant.

58. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from the Data Breach.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

59. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

60. Defendant's duty to use reasonable care in protecting the Sensitive Information arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential information.

61. Defendant breached its common law, statutory, and other duties -- and thus, was negligent -- by failing to use reasonable measures to protect students', alumni's, and applicants' Sensitive Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class Members' Sensitive Information;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiff's and the Class Members' Sensitive Information; and

d. failing to warn Plaintiff and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

62. Defendant owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

63. It was foreseeable that Defendant's failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

64. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

65. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the Sensitive Information of Plaintiff and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the Sensitive Information.

66. As a result of the foregoing, the Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of Plaintiff and the Class which Plaintiff and members of the Class were required to provide to Defendant as a condition of filing an application with HACLA.

67. Plaintiff and members of the Class reasonably relied on the Defendant to safeguard their information, and while Defendant was in a position to protect against harm from a data breach, Defendant negligently and carelessly squandered that opportunity. As a proximate result, Plaintiff and members of the Class suffered and continue to suffer the consequences of the Data Breach.

68. Defendant's negligence was the proximate cause of harm to Plaintiff and members of the Class.

69. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information of its students, alumni, and applicants, Plaintiff's and Class

Members' Sensitive Information would not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

70. However, as a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, among other things; (1) the loss of the opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiff's and the Class Members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial and/or healthcare and/or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, healthcare or medical accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their Sensitive Information, which remains in the Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

71. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

SECOND CAUSE OF ACTION
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq*

72. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

73. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

74. Defendant violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

75. Defendant's "unfair" and "fraudulent" acts and practices include omitting, suppressing, and concealing the material fact that they did not have and did not reasonably ensure that HACLA reasonably or adequately secured Plaintiff's and Class Members' Sensitive Information.

76. Defendant engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

77. Defendant engaged in acts of deception and false pretense in connection with its accepting, collecting, securing, and otherwise protecting Class Members' Sensitive Information and engaged in the following deceptive and unconscionable trade practices, including:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Sensitive Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Sensitive Information at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit its data security systems;

e. Failing to adequately monitor, evaluate, and ensure the security of its network and systems;

f. Failing to recognize in a timely manner that Plaintiff's and other Class Members' Sensitive Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiff's and Class Members' Sensitive Information had been improperly acquired or accessed.

78. Plaintiff's and Class Members' Sensitive Information would not have been compromised but for Defendant's wrongful and unfair breach of its duties.

79. Defendant's failure to take proper security measures to protect private Sensitive Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Sensitive Information.

80. Plaintiff and Class Members conferred a benefit on Defendant – assistance with finding affordable housing-- in reliance on Defendant's omissions and deceptive, unfair, and unlawful practices. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that they did not adequately secure Plaintiff's and Class Members' Sensitive Information, Plaintiff and Class Members would not have sought or purchased services from Defendant.

81. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and lost money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein.

82. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their Sensitive Information; reasonable attorneys' fees and

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

THIRD CAUSE OF ACTION
VIOLATION OF CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750, *et seq.*

83. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

84. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

85. Defendant is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

86. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

87. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

88. Plaintiff and Class Members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

89. Defendant's acts and practices were intended to and did result in the sales of products and services to Plaintiff and Class Members in violation of Civil Code § 1770, including, but not limited to omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' Sensitive Information.

90. Defendant's omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' Sensitive Information.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

91. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced employ systems with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class Members' Sensitive Information as part of the services it provided without advising Plaintiff and Class Members that their data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' Sensitive Information. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered.

92. As a direct and proximate result of Defendant's violations of California Civil Code § 1770, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Sensitive Information; and an increased, imminent risk of fraud and identity theft.

93. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

FOURTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*

94. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1798.2. The disclosure must "be made in the most expedient time possible and without unreasonable delay" *id.*, but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82, subdiv. b.

95. The Data Breach constitutes a "breach of the security system" of Defendant.

96. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

97. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class, but waited months to notify them. This was an unreasonable delay under the circumstances.

98. Defendant's unreasonable delay prevented Plaintiff and Class Members from taking appropriate measures to protect themselves against harm.

99. Because Plaintiff and Class Members were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

100. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

FIFTH CAUSE OF ACTION
INVASION OF PRIVACY

101. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

102. The Restatement (Second) of Torts states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.
>
> Restatement (Second) of Torts § 652B (1977)

103. Plaintiff and Class Members had a reasonable expectation of privacy in the Sensitive Information that Defendant mishandled. Plaintiff and Class Members maintain a

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

privacy interest in their Sensitive Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

104. Plaintiff's and Class Members' Sensitive Information was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, including Social Security numbers, that were only shared with Defendant for the limited purpose of obtaining Defendant's housing services.

105. Additionally, Plaintiff's and Class Members' Sensitive Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Sensitive Information for fraud, identity theft, and other crimes without their knowledge and consent.

106. Defendant unlawfully intruded upon Plaintiff's and Class Members' solitude, seclusion, or private affairs. Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person.

107. Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Sensitive Information was stored and disclosed private facts about them (including their Social Security numbers) into the public domain (in this case, the dark web).

108. In failing to protect Plaintiff's and Class Members' Sensitive Information, and in intentionally misusing and/or disclosing their Sensitive Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

109. Plaintiff and Class Members have been damaged by Defendant's conduct, by incurring the harms and injuries arising from the Data Breach now and in the future. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Xavier Neal-Burgin demands judgment on behalf of himself and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing the named Plaintiff to be class representative and the undersigned counsel to be Class counsel;

b. Requiring that Defendant pay for notifying the members of the Class of the pendency of this suit;

c. Awarding Plaintiff and the Class appropriate relief, including actual damages, compensatory damages, and punitive damages on the above-listed Causes of Action;

d. Awarding Plaintiff and the Class prejudgment and post-judgment interest;

e. Awarding Plaintiff and the Class their attorneys' fees and costs pursuant to applicable laws, together with their costs and disbursements of this action; and

f. Awarding such other and further relief as the Court may deem just and proper.

Respectfully submitted,

Dated: March 23, 2023

KELLER GROVER LLP

By: _____
ERIC A. GROVER
ROBERT SPENCER
Attorneys for Plaintiff

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the Class, demands a trial by jury as to all issues triable of right.

Respectfully submitted,

Dated: March 23, 2023

KELLER GROVER LLP

By: _____
ERIC A. GROVER
ROBERT SPENCER
Attorneys for Plaintiff

EXHIBIT A

Todd S. Garber

HACLA
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 10, 2023

J1405-L03-0296447 T01006 P016 **********5-DIGIT 90035
XAVIER L NEAL-BURGIN
APT 2
1431 S SHENANDOAH ST
LOS ANGELES, CA 90035-3566

NOTICE OF DATA BREACH

Dear XAVIER L NEAL-BURGIN:

The Housing Authority of the City of Los Angeles ("HACLA") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On December 31, 2022, HACLA discovered encrypted files on certain computer systems. HACLA learned that it had been the victim of a complex cyber-attack. HACLA immediately shut down its servers and launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the incident. The forensic investigation determined there was unauthorized access to certain servers between January 15, 2022 through December 31, 2022. HACLA immediately undertook a comprehensive review of all data contained on our systems that may have been the subject of any unauthorized access or acquisition. On February 13, 2023, we completed this review and determined that certain data relating to you was included in the affected servers. Out of an abundance of caution, we are providing notice to you.

What Information Was Involved? The data that relates to you and may have been affected by this incident includes your name and Social Security number, date of birth, driver's license or state identification number, government issued identification number, and military identification number.

What We Are Doing. Upon discovery of this event, we immediately commenced an investigation with third-party specialists to confirm the nature and scope of the incident. We reported this incident to local, state, and federal law enforcement agencies. Although we had safeguards surrounding data security in place at the time of the incident, we are reviewing our policies and procedures relating to data privacy and security. While we are unaware of any actual or attempted fraudulent misuse of your information as a result of this incident, we are offering you access to 12 months of complimentary credit monitoring through Experian. In addition, we are providing notice to appropriate regulatory authorities.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Personal Information*. There you will also find instructions to enroll in the free credit monitoring and identity protection services we are making available to you. While HACLA will cover the cost of these services, you will need to complete the activation process yourself, as we are unable to enroll you on your behalf.

B084813

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-800-459-4196 Monday – Friday, 6:00am to 8:00pm PT, Saturday – Sunday, 8:00am to 5:00pm PT. Be prepared to provide your engagement number B084813. You may also write to HACLA at Attention: Incident Response, 2600 Wilshire Blvd., Los Angeles, CA 90057.

Sincerely,

The Housing Authority of the City of Los Angeles

Եթե ցանկանում եք ստանալ այս նամակը հայերենով, խնդրում ենք զանգահարել 1-866-566-1362 հեռախոսահամարով և տրամադրել փոստային հասցե, և մենք այն կուղարկենք ձեզ:

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** June 30, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: 7Q4JTGSQK

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-800-459-4196 by June 30, 2023. Be prepared to provide engagement number B084813 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from the violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 57 Rhode Island residents impacted by this incident.